INTERNET OF MEDICAL THINGS: LEGAL CHALLENGES IN THE EU

Dusko Milojevic

GETS, 16-17 May, Phoenix


KU LEUVEN

AGENDA

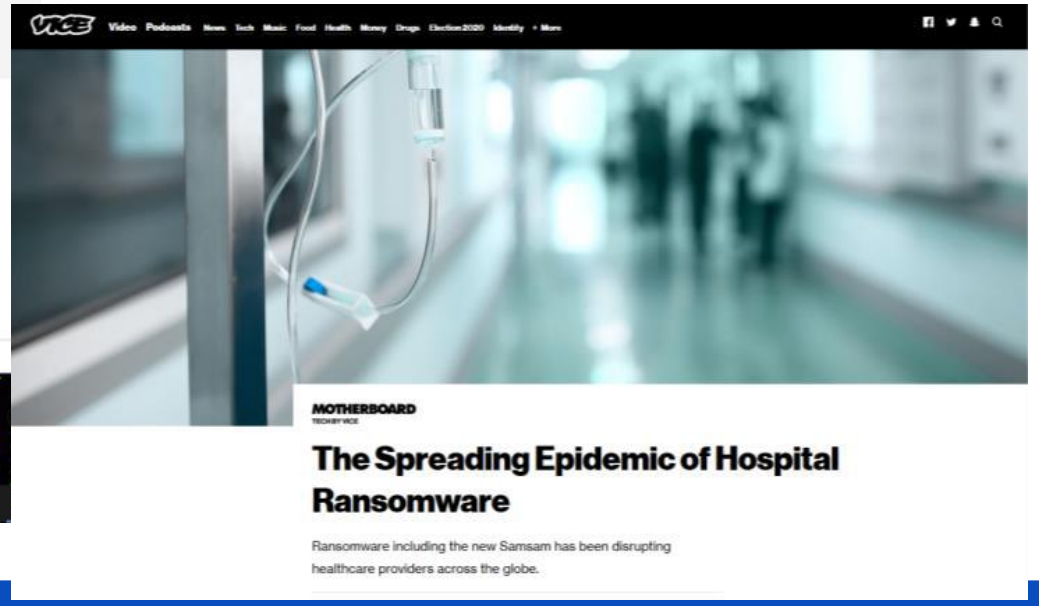
- IOMT - Intro
- EU Regulatory Landscape
- Legal Challenges
- Certification Schemes and Standards
- Conclusion

IOMT – GENERAL REMARKS

- What is IOMT?
  - Lack of consensus regarding the definition
  - Not founded in EU hard law
  - Lack of clarity over the term in complex IOMT environment hampers enhancing of cyber posture and cyber culture
- Transformative impact on healthcare
  - Remote real-time monitoring
  - Costs and time savings
  - Early prevention and diagnosis

UNIQUE CHALLENGES TO THE HEALTHCARE SECTOR

- Privacy risks
- Security risks
- Ethical concerns



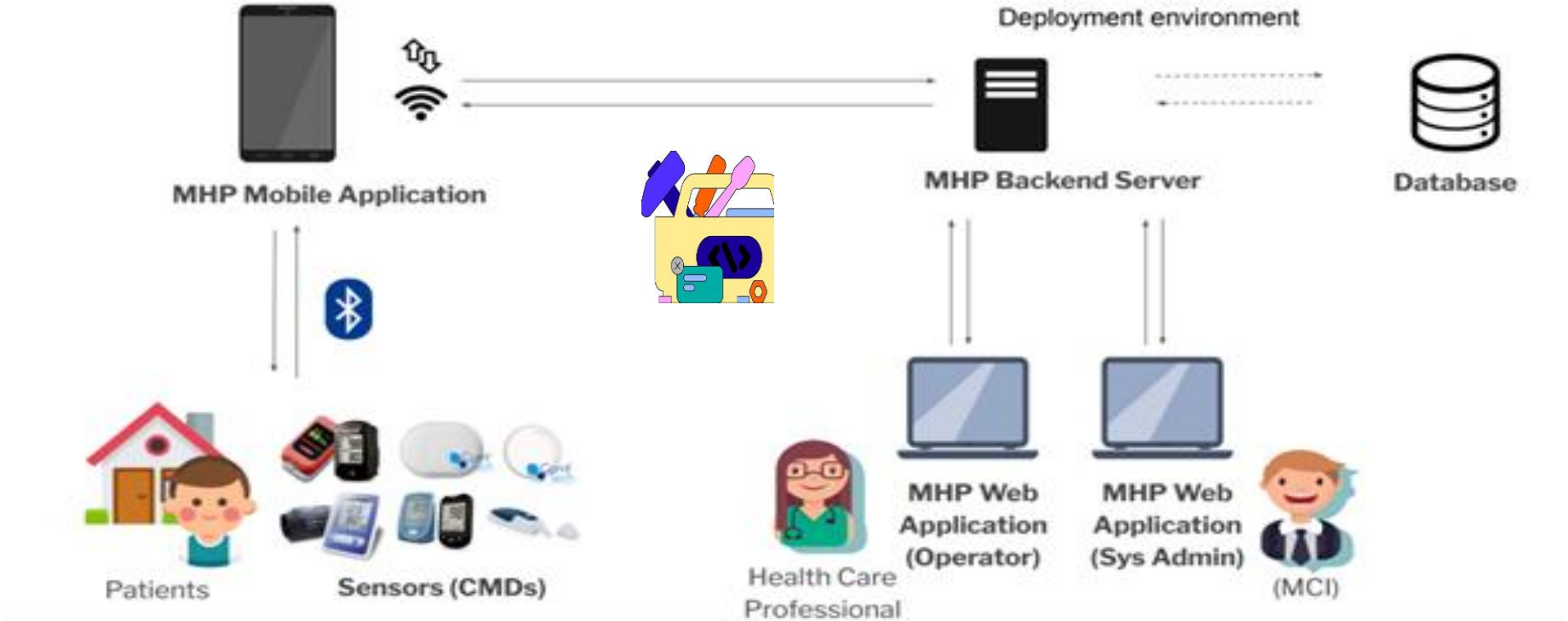
IOMT ARCHITECTURE

PERCEPTION/SENSING LAYER

NETWORK LAYER

PROCESSING LAYER

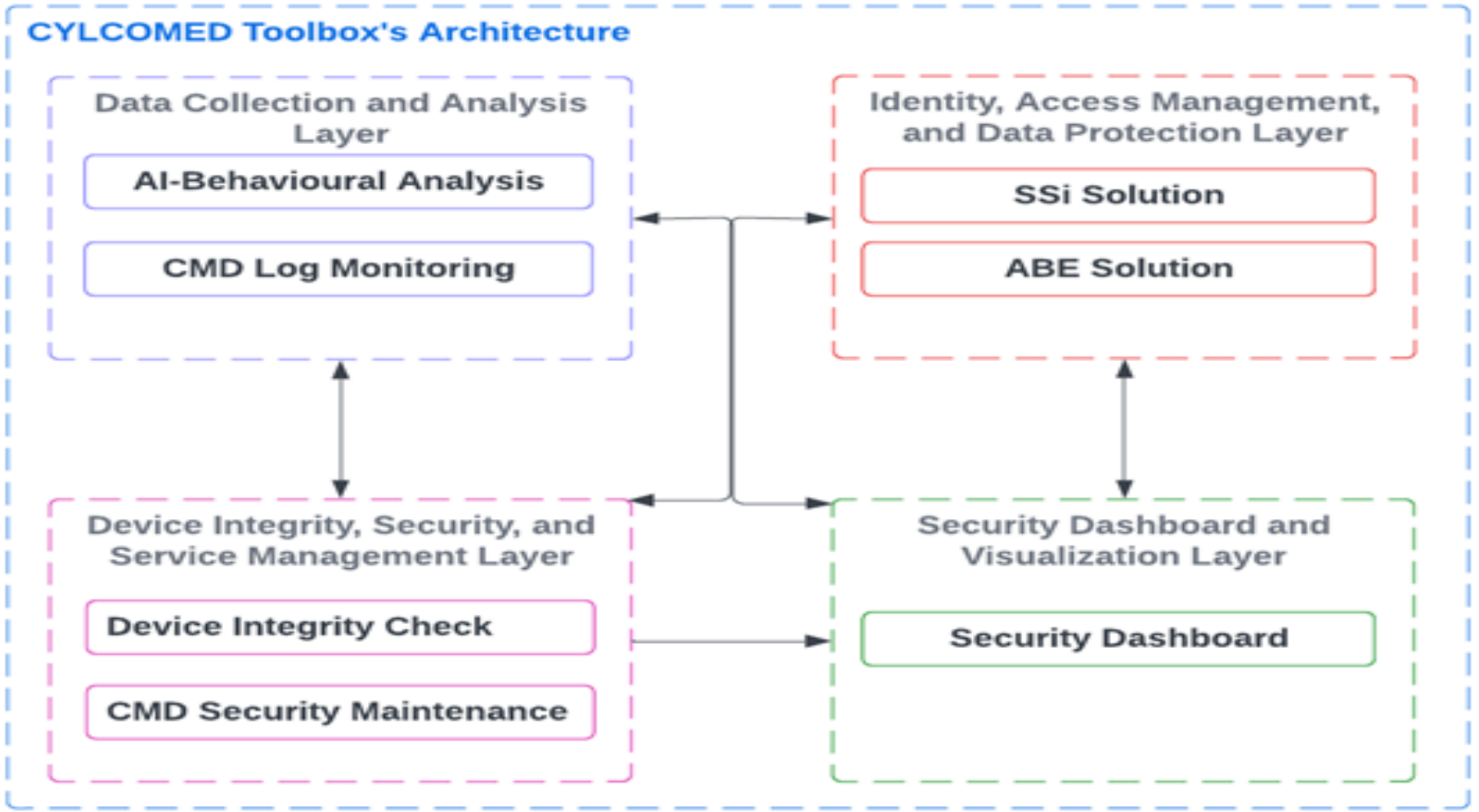
APPLICATION LAYER

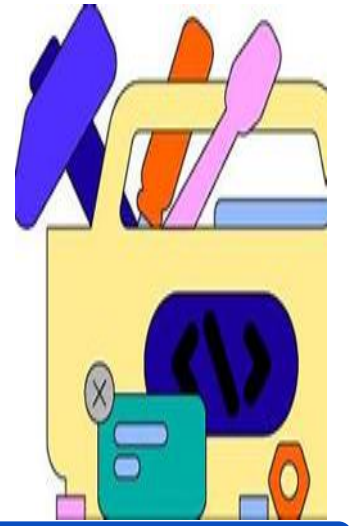


IOMT CYLCOMED PILOT

CYBERSECURITY TOOLBOX

CYLCOMED





OVERVIEW OF LEGAL FRAMEWORKS GOVERNING CYBERSECURITY OF IOMT

Data Law Framework	Cybersecurity Law Framework	AI Law Framework	Medical Devices Laws
Data Protection Law	Cybersecurity Act	AI Act	MDR
Data Act	NIS2	Soft Law Instruments	IVDR
EDHS	RED / RED Delegated Act		MDCG Guidance
	Cyber Resilience Act		

LEGAL FRAMEWORKS

GDPR

- Technical and organisational measures
- Data breach notification
- DPIA
- DPO

CYBERSECURITY ACT

- Establishes ENISA
- Introduce the voluntary cybersecurity certification scheme
- assurance levels: ‘basic’, ‘substantial’ or ‘high’

NIS2

- MS are required to adopt national cybersecurity strategies and to designate or establish competent authorities
- Technical and organisational measures
- Risk management approach
- Notification duties for essential and important entities

RED / CYBER RESILIANCE ACT

- all internet-connected radio equipment, including Internet of Things (IoT) with a radio (wireless) function and wearables (i.e., smart watches) fall under the Directive's scope
- CRA will fulfil the missing link in the cybersecurity legislative framework that will specifically address cybersecurity in products with digital elements

LEGAL FRAMEWORKS

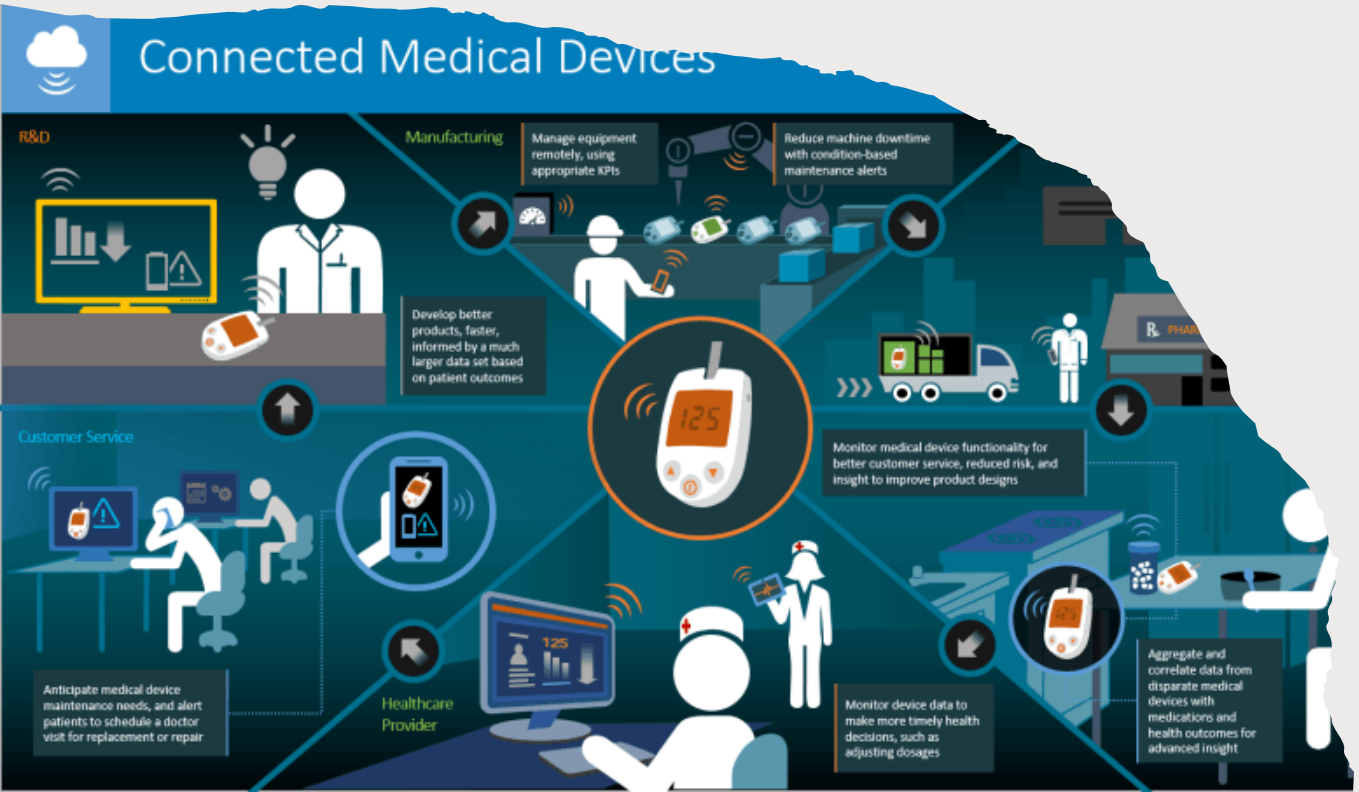
MDR/IVDR

- Central piece of legislation for connected medical devices
- Software as medical device
- Stringent requirements
- No reference to cybersecurity

AI ACT

- Adopted in 2024
- Specifically addresses cybersecurity
- Stringent requirements for deploying high risk AI systems

MDCG 2019-16 GENERAL OBSERVATIONS



- Not legally binding
- Superficially addresses connection between soft law instrument and hard law
- does not include explicit definitions nor reference to terms such as "cybersecurity," "security-by-design," and "security-by-default."
- Fails to further clarify notion of “Cybersecurity is shared responsibilities”
- No reference to ethics
- “Outdated”

LEGAL CHALLENGES

- Regulatory overlapping
- Fragmentation risks
- Regulatory uncertainty
- Duplication
- Vague formulations

DUPLICATION:
THE NOTIFICATION OF MEDICAL DEVICES SECURITY INCIDENTS

MDR	GDPR	NIS2
Serious incident notification	Data breach notification	• Security incident notification
Competent authority	Supervisory authority	• National authority or CSIRT
Immediately and not later than 15 days	Without undue delay and, where feasible, not later than 72 hours after having become aware of it	• Within 24 hours, an early warning • Within 72 hours, an incident notification

DUPLICATION: THE NOTIFICATION OF MEDICAL DEVICES SECURITY INCIDENTS

MDR

- Serious incident notification
- Competent authority
- Immediately and not later than 15 days

GDPR

NIS2

- rity incident
  ication
- nal authority or
  T
- in 24 hours, an early
  ing
- in 72 hours, an
  dent notification

AI ACT

- Serious incident
- to the market surveillance authorities of the Member States
- Immediately and not later than 15 days

THE ROLE OF CYBERSECURITY CERTIFICATION

- Potentially overlapping requirements
- Different certification schemes
- Lack of comprehensive standards in the IOMT environment

CONCLUSION

CONCLUSION

- The IoMT has the potential to transform healthcare, but it is essential to address the significant cybersecurity and privacy risks associated with this technology

- EU cybersecurity legislative framework is quickly developing and becoming ever more complex

- Cybersecurity standards could play a critical role in increasing harmonisation, introducing actionable requirements, and increasing legal certainty.

CYLCOMED

THANK YOU FOR YOUR ATTENTION

cylcomed.eu

Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**